This document is published in:

Bossé, E. et al. (eds.), 2013. *Prediction and Recognition of Piracy Efforts Using Collaborative Human-Centric Information Systems*, Proceedings of the NATO Advanced Study Institute (ASI), Salamanca, Spain 19-30 September, 2011, (NATO Science for Peace and Security, Sub-Series - E: Human and Societal Dynamics, v. 109), IOS Press, pp. 80-88.

DOI: 10.3233/978-1-61499-201-1-80

# Contextual Knowledge and Information Fusion for Maritime Piracy Surveillance

Jesus GARCIA[a], Galina ROGOVA[b, 1]
[a]*University Carlos III of Madrid, Madrid, Spain*
[b]*Encomass Consulting, Honeoye Falls, NY, USA*

**Abstract.** Though piracy accounts for only a small fraction of the general losses of the maritime industry it creates a serious threat to the maritime security because of the connections between organized piracy and wider criminal networks and corruption on land. Fighting piracy requires monitoring the waterways, harbors, and criminal networks on the land to increase the ability of the decision makers to predict piracy attracts and manage operations to prevent or contain them. Piracy surveillance involves representing and processing huge amount heterogeneous information often uncertain, unreliable, and irrelevant within a specific context to detect and recognize suspicious activities to alert decision makers on vessel behaviors of interest with minimal false alarm. The paper discusses the role of information fusion, and context representation and utilization in building an piracy surveillance picture.

**Keywords.** Piracy threats maritime surveillance, context, reasoning, ontologies

## Introduction

According to the International Maritime Bureau's (IMB) Piracy Reporting Center piracy has been on the rise for years. There are multiple reasons for this such as [2]:

- limitless range of vulnerable targets, enormous volume of commercial ships;
- the need for ships to pass through congested (and ambush-prone) choke points;
- vast territorial waters;
- skeleton crews;
- limited resources for monitoring territorial waters and ports;
- lack of international laws;
- corruption and easily compromised judicial structures;
- situation in Somalia;
- willingness of ship owners to pay ransom;
- limited inter-government cooperation, etc.

Although piracy accounts for only a small fraction of the general losses of the maritime industry it creates a serious threat to the maritime security due to the connections between organized piracy and wider criminal networks, and corruption on land. Specifically piracy represents direct threat to the lives and welfare and direct economic impact (fraud, stolen cargos and delayed trips and could undermine a

[1] Corresponding Author: Galina Rogova, Encompass Consulting, 9 Country Meadows Drive Honeoye Falls NY 14472, USA E-mail: rogova@rochester.rr.com

maritime state's trading ability); undermining and weakening governing legitimacy by encouraging corruption; and can lead to major environmental disaster.

Piracy as an economically driven phenomenon has specific goals and characteristics, which may be different, form ones of maritime terrorism. At the same time there are multiple similarities between them [7]. They use the same opportunities due to similar vulnerable targets caused, e.g., by the enormous volume of commercial ships, congested choke points.; or may use similar tactics. For example terrorists could hijack ships carrying huge loads of highly flammable materials to undertake a suicide mission or to ram a hijacked vessel against the container terminal or an oil refinery. Piracy and terrorist attacks are carefully planned and orchestrated, both types require significant resources and well organized crime/terrorist rings. Both terrorists and pirates use small boats, which are not much different from fishing boats. Thus the surveillance means and methods developed for asymmetric warfare and vastly published in the literature may be used for building a maritime surveillance picture. At the same time the means and methods for maritime surveillance have to be considered in the piracy context to be in order to be usable.

The process of constructing a dynamic surveillance picture for piracy threat detection and recognition involves contextual reasoning about the observed objects, processes, and events, as well as relations between them with respect to particular goals, capabilities, and policies of the decision makers. In this paper we elaborate on the role of information fusion, and context representation and exploitation in building such surveillance picture. The paper is organized as follows. Section 1 provides an introduction to the piracy problem and the role of information fusion processes in building a surveillance picture. Section 2 focuses on context definition and representation. Section 3 depicts a context based reasoning process for threat detection and recognition, and discusses possible approaches to its implementation. Finally, Section 4 presents conclusions.

## 1. Piracy threat surveillance and information fusion

"In a world where small water craft can be turned into weapons against navy destroyers and pirates can hold ships for ransom, surveillance of the sea is of increasing importance. Because of the very large area to keep under surveillance resources are inadequate to monitor the world's shipping channels, tools that help maritime surveillance analysts identify suspicious activity are extremely valuable."[9]

Detection and recognition of suspicious activity requires utilization of all available information (sensors, intelligence, and operational information) for monitoring the most vulnerable entities and facilities (such as commercial ships, harbors, linked coastal areas, etc). Exploitation of this information for building a reliable surveillance picture to support an analyst is complicated by many factors including:

- Large and heterogeneous area
- A large number of heterogeneous vessels, ranging from small recreational sailboats, tug boats and jet skis, to big commercial and cargo vessels.
- Multiple distributed decision makers from diverse agencies and different countries, with different goals, functions, and information requirements.
- Abundant available knowledge on regulations and predefined behavior of the vessels.

- Presence of distributed, uncertain, low fidelity, unreliable, irrelevant, and redundant transient information.

The key technology for building a surveillance picture is information fusion, a set of interrelated processes dealing with data and information at different levels of abstraction to produce:

- information about a single entity of interest by continuous detection, identification, tracking and tracing of vessels with observation systems (lower level fusion);
- knowledge about situation and threat (higher level fusion).

Given the aforementioned challenges, the surveillance processes must include all fusion levels. Lower level fusion must combine sources of data and information to provide unified and reliable tracking and recognition of all interesting entities. Usual technologies include vessel traffic service, coastal radars, electro-optical/infrared sensors, AIS system, etc, whose complementary nature allows enhancing the performance of each technology. For instance, GPS/DGPS accuracy and velocity data can to improve radar tracker estimates. To do that, it is necessary to conduct alignment, correlation and combination of all available information in a common spatio-time reference system.

The goal of higher level fusion is to transform information about vessel identity and tracks into knowledge about potentially suspicious behavior to aid the operator in recognition of this behavior as threat or false alarm. This knowledge is based on inferred relationships between physical entities considered in a specific context, which is continually being refined as data and information arrives. Contextual information such as traffic configuration, restricted area, maritime rules, coordinated operations, etc., is an essential information to improve these aspects of surveillance.

Previous works have suggested to use the contextual knowledge (configuration and features maps) to minimize the impact of clutter areas, missed detections, loss of resolution in high density areas such as docking areas, etc.). In [1, 3], some examples are given to tune the tracking algorithms and its parameters to adapt to the regions (sea, coast, earth). Other studies [5,14] propose to refine the model for vessel track prediction by taking into account channel configuration, allowed or preferred routes, presence of geo-coded coastal points and navigation aids, limitations derived from channels depth, excluded areas, etc. However, the methods used to improve the result of lower level fusion with contextual knowledge have to go beyond the only utilization of *a priori* information. Better interpretation of sensor data for more reliable tracking and vessel recognition should also use dynamic representation of situation allowing for context refinement and discovery. Thus dynamic interaction between lower and higher level fusion should be used to improve the fusion process at all levels. The next section will discuss the problem of context representation and exploitation in more detail.

## 2. Context representation

Context is defined by the Webster dictionary as "the events or circumstances that form, or influence, the environment, within which something exists or takes place." This definition points out to two different context paradigms introduced in [6] and further discussed in [13]. These paradigms correspond to two different but complementary views on context: in the "*Context of X"* (CO) and "*Context for X*" (CF).

The reference item X represents "any physical or conceptual entity and event" such as, e.g., a speed boat."

CO is a part of the environment, which represents a set of items and relationships "grouped or contained by X." We have certain expectations about X based on CO, e.g. in the context of situation in Somalia we can expect easy recruitment of potential pirates. Expectations defined by CO can be used for detection of possible threat based on expectations about observations obtained by surveillance evolving crisis (e.g. normal boat speed). Deviations from expected situational items and relations between them may alert decision makers and can initiate causal reasoning for discovery of a possible cause explaining such deviations. Knowledge about CO also offers predictions of the dynamics of current observations or pirate actions (e.g., in the context of willingness to pay ransom). Constrains goals, objective, functions, actions of the threat responders (what can be done given relations between countries in Malacca Strait).

Alternatively, CF defines the contextual space of items externally related to and referenced by X: the weather provides a *context for* the level of reliability of observations. Situation assessment processes use CF to better understand reference items and relations between them. Decision makers have to take CF into consideration to optimize actions. For example, the time of the day may change deterrence actions.

A set of items and relations of interest (the reference items X) constitutes the problem variables. A set of items and relations defining a CF can be called context variables. Context variables represent auxiliary variables. They affect knowledge about problem variables, reasoning about them and, therefore, decisions and actions based on the characteristics and behaviors of problem variables. Context variables may be both static (e.g., a port map) and dynamic (e.g., weather).

Context should be considered at different levels of granularity due to the distributed nature of the problem. Following [12, 13] we shall survey the context models most applicable to information fusion: (a) *Key-Value Models,* (b) *Ontology-based models,* and (c) *Logic-based models. Key-Value Models* are the simplest way of representing context. They provide values of context attributes as environmental information and utilize exact matching algorithms on these attributes. These models may suffice for use in Level 1 fusion, but they lack capabilities for complex structuring required by higher level fusion. *Ontology-based models* provide a formal and uniform way for specifying core concepts, sub-concepts, facts and their inter-relationships to enable realistic representation of contextual knowledge for reasoning, information sharing and reuse. At the same time ontologies do not support uncertain, unreliable, and imprecise context representation inherent to the piracy surveillance problem [4]. *Logic-based models* represent context as facts and information inferred from rules. The dynamic uncertain harbor surveillance scenario calls for a hybrid context representation combining ontology and logic based models enriched by uncertainty consideration.

In the case of maritime domain (including piracy), the context representation should integrate all dynamic information obtained as a result of: (i) vessel traffic information systems, such as pre-planned arrivals, ship mooring arrangements, and data from approach-speed and mooring strain sensors; (ii) IMO (International Maritime Organization) security protocols, including that coming from AIS (Automatic Identification Systems), ISPS (International Ship and Port Facility Security) codes, ship-to-shore alarms, and security and inspections. The knowledge to be considered may comprise the description of maritime (and harbor) areas and navigation restrictions expressed in general terms as a certain set of rules, comprising additional external knowledge such as applicable regulations and vessel traffic service manuals. For

instance, we can consider the following general traffic rules [4] as part of context representation:

- ***Identification****: ships entering/leaving the harbor must have a permission of Harbor Authority: destination, arrival/departure times, passengers/cargo*
- ***Speed limit****: The speed limit usually is defined for areas, lower in inner parts and higher outer. Typical values may be 5-10 knots within the harbor areas*
- ***Navigation****: there are predefined limited areas for different categories of vessels. Crossing generally forbidden*

The knowledge of all applicable rules can be essential to understand the situation and evaluate the normalcy of operations. In addition some regulated procedures, can be used to decide if the set of entities are exhibiting expected behavior. For instance specific harbor norms for special types of ships like oil containers require to follow towage/guidance boats along the harbor channels, this knowledge may explain complex ineteraction among tracked entities. Finally, it is essential to take into account that information required to understand how the vessels follow these rules can be incomplete, erroneous, uncertain, ambiguous or approximate.

## 3. Reasoning about pirate threat

Ontologically threat can be defined as a tri-part integrated whole (viable threat) and a two part integrated whole (potential threat). The parts or members of threats are often extended over spatial regions or temporal periods, dispersed wholes, which nonetheless contain parts or members that stand to one another via a certain unifying feature or characteristic of that whole and require more complex reasoning about their spatial-temporal relationships than unitary wholes [8]. Building piracy surveillance requires monitoring and detecting the parts of threat, their characteristics, behavior, and spatio-temporal relations between them in a specific maritime piracy context to identify potential threat (unitary or dispersed) and its dynamics to identify imminent threat.

For example potential threat monitoring may require tracking small arm trafficking (capability monitoring), unusual coordinating activity in the land contacts (intent monitoring) and their temporal relation (within the same time interval). Surveillance of high vulnerability areas (e.g. chocking point) can me an example of imminent threat if, for example, decision makers were alerted on existence of a potential threat.

The process of reasoning for detection and recognition of piracy threat and the role of context in this process is shown on figure 1. In this process, reasoning in the uncertain piracy surveillance environment requires:

- Detection of possible inconsistency between expected corresponding to “no threat” situation, and observed objects, relations, situational items, and their behavior
- Understanding the source of inconsistency, i.e., whether this inconsistency is the result of insufficient quality of contextual knowledge, observations, fusion processes or potential or immanent threat is discovered

Inconsistency detection may be based on explicit “normalcy” or anomaly models by using: values of characteristics or behavior of situational items obtained from the domain knowledge, rules (e.g. presence or absence of certain characteristics), hypothesis testing. Both types of these methods have some drawbacks.

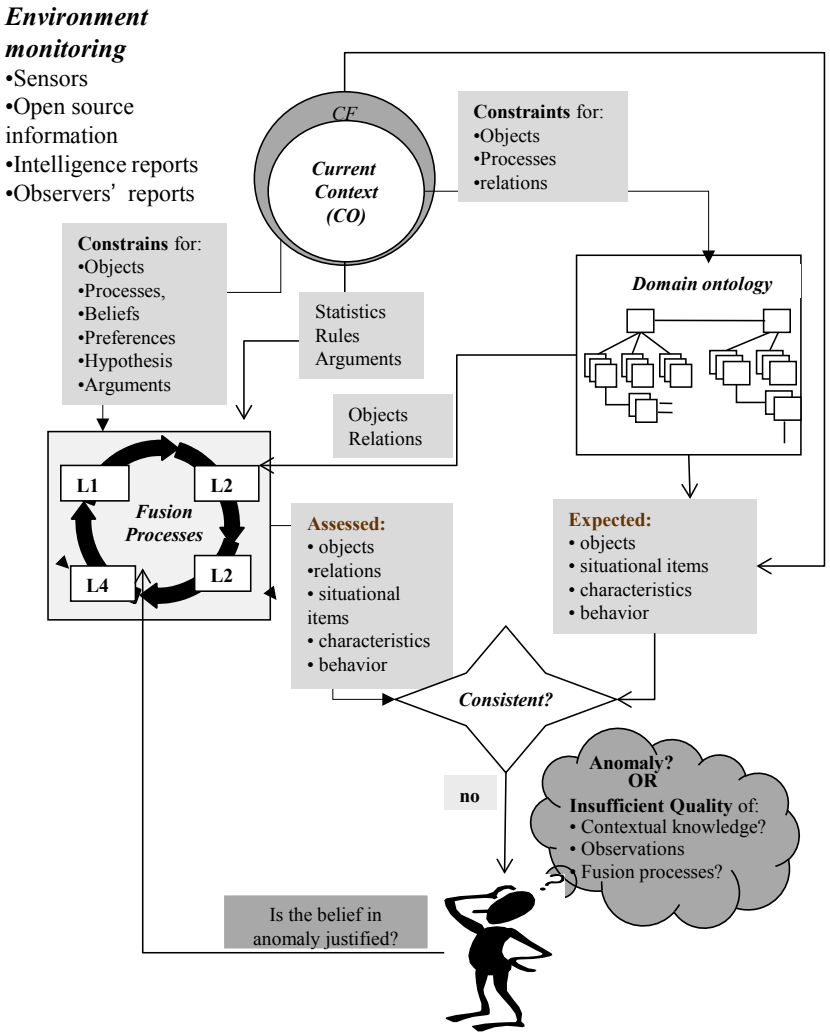


Figure 1. The reasoning process for detection and recognition of piracy threats and the role of context

Thus building a normalcy model may have a scalability problem (to many normal situations) while abnormal behavior can encounter the "black swan problem". Another methods relay on incremental learning operating on evolving data ("on-line" stream classification problem"). These methods can identify unseen earlier patterns of behavior or characteristics but may encounter the situation, in which a pattern considered as anomaly could become normal when more information is available.

Reasoning for explaining the source of inconsistency (abduction) can be of two types: qualitative, in which uncertainty is handled by manipulation of symbols and quantitative, in which uncertainty is encoded by numbers. At the same time no such

method is able to deal with all types of uncertainty and utilization of hybrid approaches are required.

One of the hybrid paradigms that can be considered for abductive uncertain reasoning proved itself in threat detection is the Belief-based Argumentation System (BAS) [10], BAS is an approach to non-monotonic reasoning under uncertainty, combining symbolic logic with belief theory for judging hypotheses about the unknown or future world by utilizing given knowledge. Logic is used to find arguments in favor of and against a hypothesis about possible causes or consequences of the current state. An *argument* is built on uncertain assumptions that make the hypothesis true, or false. Every assumption is linked to *a non-additive belief* that the assumption is true or false. The beliefs that the arguments are valid are used to compute the credibility of the hypothesis, which can then be measured by the total belief that it is supported by the totality of supportive and refuting arguments. The resulting degree of support corresponds to belief of the theory of evidence and is used to make a decision whether a hypothesis should be accepted, rejected, or whether the available knowledge is insufficient to form a satisfactory judgment at this time. The beliefs assigned to the assumptions can be expressed in linguistic form; e.g., very high, high, low, very low with subsequent quantization of these linguistic values. The beliefs can be also represented numerically and be approximated by a function of the values assigned to attributes and relationships characterizing the state of environment and related to the assumptions. In some cases these belief measures can be the result of a combination of beliefs based on different characteristics with the Dempster rule [11]. Arguments and assumption can be provided by ontological reasoning through definition of contextual, heuristic, and common sense conditions that activate an interesting situation in the piracy surveillance scenario.

The following example illustrates the application of the BAS to recognition of possible threat from a boat [4]:

- Boat features (speed, direction, type, flag, etc.)
- Spatio-temporal relations between the suspicious boat and others, or relations between the boat and harbor zones
- Beliefs assigned to assumptions are based on the observed spatio-temporal relations and correspondence of the boat behavior to rules and regulations

One of the arguments *pro* hypothesis "treat" from a vessel can be built as a conjunction of the following uncertain assumptions:

A1: the suspicious boat is too close to a vessel sailing in the opposite direction.

A2: The vessel following in the opposite direction is a big cruise ship.

A3: The suspicious boat is increasing its speed.

Each assumption is assigned a belief measure, representing belief that this assumption is true. In our example these belief measures are modeled as functions of the behavior of suspicious vessel characteristics (increased speed), type of the vessel following in the opposite direction, and relation "close" between the suspicious vessel, a vessel following in a different direction. Thus, the belief in "too close" can be measured as a function of (1) the difference between the distance observed and the distance allowed for consideration big cruise ship, and (2) the accuracy and reliability of the distance observed.

## 5 Conclusions

The maritime piracy threat detection and characterization requires exploitation of advanced information fusion processes, which must be adaptive and context-sensitive. This paper has discussed some aspects of designing such processes, including contexts representation and exploitation and possible approach to reasoning under uncertainty adapted to maritime piracy surveillance domain.

There are many open questions related to designing an operational surveillance system for assisting an operator in piracy threat recognition and deterrence. Some of them are associated with hybrid context representation combining ontology and logic based models incorporating uncertainty with an appropriate trade-off between completeness and complexity, formal aspects to model anomaly and context dynamics. Another challenge is an effective integration of such contextual representation at all fusion levels.


## Acknowledgements

This paper has utilized the results of the research activity supported in part by Projects CICYT TIN2008-06742-C02-02/TSI, CICYT TEC2008-06732-C02-02/TEC and CAM CONTEXTS (S2009/TIC-1485)


## References


[1] A. Benavoi, L. Chisci, A. Farina, S.Immediata, L. Timmoneri. Knowledge-Based System for Multi-Target Tracking in a Littoral Environment. IEEE Trans. on Aerospace and Electronic Systems. V. 42, N3, 2006. 1100-1119

[2] P. Chalk: Maritime Piracy: Reasons, Dangers and Solutions, 2009, http://www.rand.org/pubs/testimonies/2009/RAND_CT317.pdf

[3] J. García, J.L. Guerrero, A. Luis y J. M. Molina. "Robust Sensor Fusion in Real Maritime Surveillance Scenarios", 13th International Conference on Information Fusion, Edinburgh, UK: July 26-29, 2010.

[4] J. Garcia, J. Gomez-Romero, M.A. Patricio, J.M. Molina, G.L Rogova, On the Representation and Exploitation of Context Knowledge in a Harbor Surveillance Scenario, in*: Proc. of the Forteenth International Conference on Information Fusion, Chicago, 2011.*

[5] J. George; Crassidis, J.L.; Singh, T. "Threat assessment using context-based tracking in a maritime environment" 12th International Conference on Information Fusion. Seattle, WA 6-9 July 2009

[6] L. Gong, "Contextual modeling and applications," *Proc. IEEE International Conference on SMC, V1, 2005.*

[7] S Hanson, Combating Maritime Piracy, 2010, http://www.cfr.org/france/combating-maritime-piracy/p18376

[8] E. Little, G. Rogova, An Ontological Analysis of Threat and Vulnerability, in: *Proc. of the FUSION'2006-9th Conference on Multisource Information Fusion*, 2006.

[9] NURC. http://www.nurc.nato.int/research/msa.htm

[10] G. Rogova, P. Scott, C. Lollett, and R. Mudiyanur, Reasoning about situations in the early post-disaster response environment, *9th Int. Conference on Information Fusion, 2006, Florence, Italy*.

[11] G. Shafer, *A Mathematical Theory of Evidence*, 1976. Princeton University Press, 1976

[12] T. Stang, and C. Linnhoff-Popien, A context modeling survey, *1st Int. Workshop on Advanced Context Modeling, Reasoning and Management,* 2004, Nottingham, UK.

[13] A.N. Steinberg and G.L. Rogova, "Situation and context in data fusion and natural language understanding," *Proc. of the Eleventh International Conference on Information Fusion, Cologne, 2008.*

[14] M. Vespe, M. Sciotti, F. Burro, G. Battistello, and S. Sorge Maritime multi-sensor data association based on geographic and navigational knowledge. IEEE Radar Conference, 2008.